CONF-801113--2

LA-UR-80-1617

38

TITLE: THE LOS ALAMOS SCIENTIFIC LABORATORY LONG-RANGE ALARM SYSTEM

AUTHOR(S): Robert DesJardin and Jack Machanik

SUBMITTED TO: 1980 International Conference:
Security Through Science and Engineering
Berlin, Germany
September 23-26, 1980

THE LOS ALAMOS SCIENTIFIC LABORATORY LONG-RANGE ALARM SYSTEM

by

Robert DesJardin
University of California
Los Alamos Scientific Laboratory
Los Alamos, New Mexico 87545 USA

and

Jack Mashanik
Bradford National Corporation
New York, New York 10057 USA

Abstract. This paper presents a description of the Los Alamos Scientific Laboratory (LASL) Long-Range Alarm System to the security community.

The last few years have brought significant changes in the Department of Energy regulations for protection of classified documents and special nuclear material. These changes in regulations have forced a complete redesign of the LASL security alarm system.

LASL covers many square miles of varying terrain and consists of separate technical areas connected by public roads and communications.

A design study over a period of 2 years produced functional specifications for a distributed intelligence, expandable alarm system that will handle 30,000 alarm points from hundreds of data concentrators spread over a 250-km² area. Emphasis in the design was on nonstop operation, data security, data communication, and upward expandability to incorporate fire alarms and the computer-aided dispatching of security and fire vehicles.

All aspects of the alarm system were to be fault tolerant from the central computer system down to but not including the individual data concentrators. Redundant communications lines travel over public domain from the alarmed area to the central alarm station.

Introduction

The Los Alamos Scientific Laboratory (LASL) is presently upgrading its security alarm system. This upgrade was made necessary through a combination of changes in Department of Energy (DOE) specifications and the outdated condition of the existing 30-year-old alarm system.

A description of the existing alarm system and the objectives of the Long-Range Alarm System (LORAX) were previously covered in a paper presented at the Carnahan Conference on Crime Countermeasures.[1]

System Overview

The LORAX system is funded as a part of the DOE Safeguards program. The Safeguards program covers the upgrading of physical protection and nuclear material accountability as well as alarm systems.

To meet the performance goals, a system architecture was developed and is illustrated in Fig. 1. The divisions at the top of the figure represent the major system functions; that is, field installation, including an intelligent multiplexing system that concentrates the alarm data, the central alarm station; and the remote man/machine interface terminals (operator stations).

If a sensor is triggered or a tamper is detected, an alarm is transmitted over the data communication system to the central computer system located at the central alarm station. The computer will identify a response preplanned for the alarm and transmit it to the DOE Dispatch Station 100. Emergency phone calls are handled through the 911 telephone system. When a 911 call is received, the DOE operator fills out a CRT form that creates an alarm event. The DOE response forces can be dispatched through a computer-aided dispatch system or telephone.

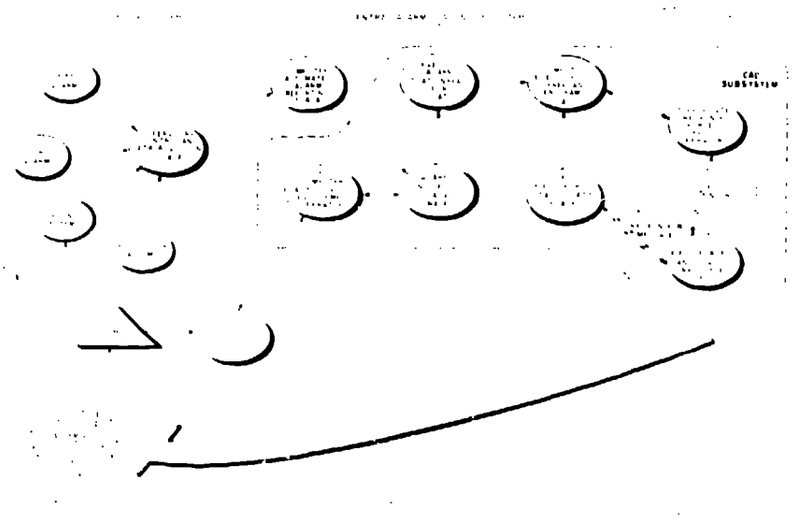

Figure 1. LORAX system overview.

Because of the size of the security upgrade program, the LORAX system is being developed in two phases. The first phase, which is strictly security, will include all of the functions illustrated in Fig. 1 with exception of computer-aided dispatch. Software hooks will be made available and the computer-aided dispatch will be added at a later date. In the interim, response forces will be manually dispatched through telephone or existing radio channels.

Specific LORAX Security Activities

Specific operational activities that are monitored, assisted, or controlled by the LORAX system and its operators are as follows:

- Monitoring status of all intrusion detection system (IDS) sensors, that is, access/secure, alarm, tamper and line faults.
- Monitoring and controlling all personnel authorization and supervision subsystems; that is, access/secure, badge/card readers, keyboard entry ID, guard watch tours, duress alarm, and local annunciators.
- Monitoring and controlling all IDS tests.
- Monitoring status of the IDS response force.
- Presenting response force preplans corresponding to alarm incidents.
- Correlation of alarms that may be from the same incident.
- Conducting computer-aided dispatch and supervision of the IDS response force.
- Maintaining IDS operational and archival records, logs, reports.
- Access/secure log.
- Printout of all IDS alarms with resulting IDS response force actions and statements of incident resolution.
- Recording of all IDS radio transmissions.
- Records of all IDS local and remote test results.
- Personnel access activities log.

LORAX Software Overview

LORAX software is distributed and multilayered. Distributed implies that executable code and data reside in discrete and separate components of the system, that is, the central computer, the field concentrators, and in intelligent terminals. Multilayered means the software is arranged in a hierarchical structure. The operating system software supplied by Tandem Computers, Inc., provides various facilities for file management and data communications, the LORAX executive programs add utilities for line and screen handling, and finally the application programs implement the various facets of plant security protection. Software at each level has been structured into functional modules facilitating back-up procedures which insure nonstop operation of the system, as well as to allow for future growth. Planning is underway to add fire protection services to the LORAX system for the LASL complex and its adjacent community.

Whenever possible, the LORAX software has been designed to take advantage of the unique architecture of the Tandem computer and its ancillary operating software. For example, each process executing in the central computer is backed up by a process in a different processor/memory unit. Tandem processes consist of a program area and a separate data area. The program area is pure code; therefore only the data need to be saved at critical stages of the operation. The Tandem operating system provides facilities for monitoring the health checks of each central processing unit (CPU). The appropriate back-up process is initiated in the event of a CPU failure with minimal disruption of the process flow. All system and application programs in the central computer are written in TAL, which is an Algol-like, block-structured language. The TAL compiler generates

the reentrant program code so that several copies of a process can operate simultaneously using the same memory locations, each with its own data area in memory. By applying enqueueing techniques to common files, it is possible to implement multi-threading of process tasks within the LORAX environment. In other words, several alarms can be handled simultaneously by the software on a priority driven interrupt basis.

A centralized data base furnishes the key to the integration and operation of the distributed LORAX software. Within the Tandem system, tables keep track of on-going processes as well as the location of system resources to provide for optimal operations and for back-up and restart procedures. The LORAX data base is implemented through Tandem's file management system and provides multikey access to the diverse elements of the security system. Executable code and data are downline loaded from the central data base to the field concentrators and to intelligent terminals. Messages from these remote sites are in turn linked through the data base to the appropriate security response and logging functions. Management reports are generated from the data base through the use of the Tandem query and report generation software package.

Software in the field concentrators is used to perform three discrete functions within the LORAX system.

1. Control the interaction between clusters of CRT terminals, printers, and other man-machine interface devices to the central computer.

2. Interface on-line information to and from other Los Alamos computers and the LORAX system.

3. Provide all site security functions, including intrusion alarm detection reporting and site access control.

The appropriate set of object modules and data tables are downline loaded from the central computer to each field concentrator to implement the required functions at the remote site. New microprocessor codes for the field concentrators is generated on a development system and loaded into the Tandem computer through a serial port where it is stored for subsequent use. If there is a temporary loss of communication with the central computer, the concentrator software associated with site security is capable of implementing a reduced set of functions in a standalone mode.

Security Considerations

Security considerations for the LORAX system can be divided into three areas:

- Security internal to an alarm-protected area.
- Transmission of the data from the alarm-protected area to the central alarm station, and in turn transmission of the alarm preplans to the operator's terminals.
- Security internal to the central alarm station.

Security Internal to the Alarm-Protected Area

All security sensors, whether they are door switches, motion detectors, badge readers, etc., are monitored by the SCADA multiplexor unit, illustrated in Fig 2. The multiplexor has special security function cards that perform a dc supervision of each sensor. The supervision will produce four different alarm states:

- Tamper alarm -- all sensors and multiplexor cabinets contain tamper switches.
- Real alarm -- the sensor itself has been triggered.

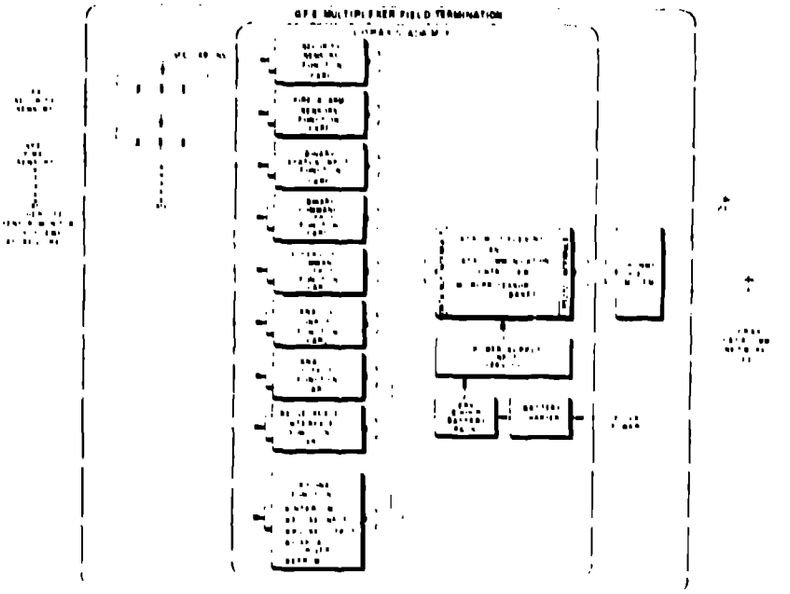

Figure 2. LORAX multiplexor.

- Line fault -- the line is short circuited (treated as a tamper).
- Line fault -- the line is open circuited (treated as a tamper).

The supervision tolerance is such that an alarm will be generated with a 6% change in the dc current level. The data inputs to the multiplexors are scanned at least every 100 ms by the multiplexor, and any change of state is latched and buffered to be sent to the central alarm station. When an alarm is generated, the multiplexor will issue a signal to the central alarm station indicating that it wants to be polled. In addition to the electrical supervision of the sensors, the multiplexor itself is located within the alarm-protected area and is under the premise control of the roving Protective Force.

Transmission to the Central Alarm Station

The alarm data are transmitted to the central alarm station at the time the multiplexor is polled. The transmission protocol involves a unique Seed/Response mechanism in which a seed pattern of 8 bits is sent to the multiplexor by the central computer, and the multiplexor operates on that seed with an algorithm contained within the multiplexor. The algorithm uses the 8-bit seed pattern plus previous transmissions and other data amounting to 64 bits of information that is rearranged. The multiplexor then transmits an 8-bit response and a seed of its own to the central alarm station. The central computer compares the response with what it has computed, using the same algorithm to indicate that a valid response has been obtained. The algorithm used by the multiplexor is unique to that multiplexor, and there are up to 10 algorithms in each multiplexor that can be called to operate on the data by the central computer system. Part of the seed generation is to do an "exclusive or" so there is no repeating of the bit pattern. Redundant communication lines are used between each remote multiplexor and the central alarm station. The redundant lines are used for reliabilility. The data that are transmitted also contain a 16-bit CRC check. The protocol between the multiplexors and the central alarm station is asychronous and operates at baud rates up to 9600.

The alarm message transmissions to the operator stations contain the same security checking as between the central alarm station and the multiplexor.

Security Internal to the Central Alarm Station

The central alarm station is under supervised control 24 hours a day, 365 days a year. There is no attempt made to prevent the knowledgeable person from getting into the computer system if he has access to the central alarm station; however, all remote terminals that connect to the central alarm station have a logical line associated with them, which allows them to interact only under certain application programs. In no cases are external terminals allowed to control critical parts of the system data base. The software operating system has multiple levels of security such that changes to programs can only be obtained by the use of the appropriate "log on" code words.

Personnel Access Control

One of the requirements of the LORAX system is that it must be able to talk directly to standalone site computers as well as the SCADA multiplexors, illustrated in Fig. 3. Personnel control is typified on this diagram by a badge being read through an access control unit. The card information will be sent to a local standalone computer system that will authorize access to the appropriate area. In the event that the person is not in the local data base, the access request will be transmitted to the central alarm station to determine if the person can be granted access authorization. In the event of lost or stolen badges or additions to data bases, information is downloaded from the central alarm station to the local site controller.

A variation of access control is when an access request comes from a security area in a secure state. This request requires an access/secure switch change and is also illustrated in Fig. 3. If the appropriate badge and ID codes are read into

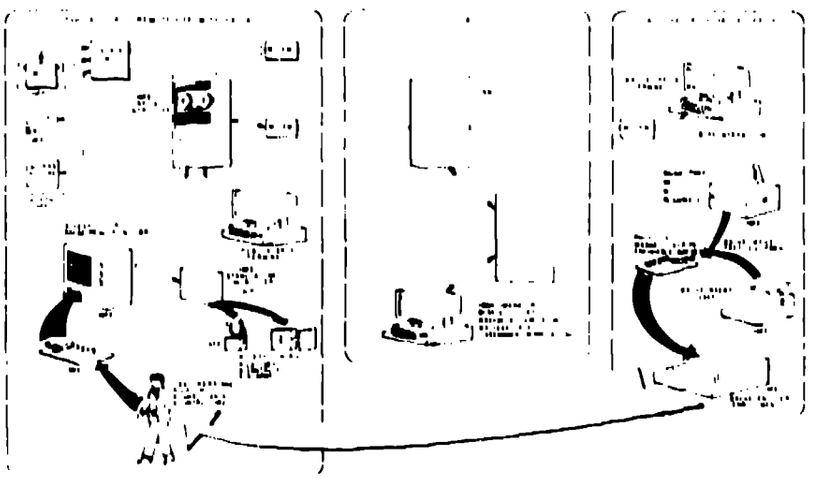

Figure 3. Access control.

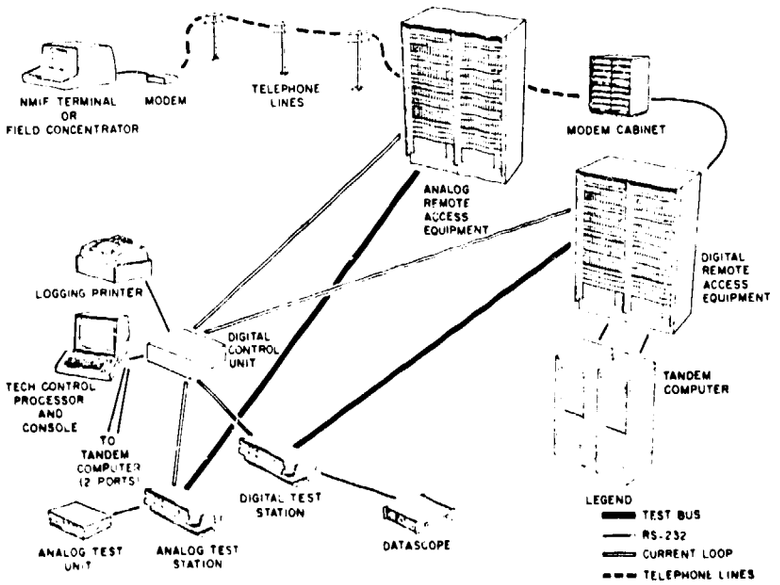

Figure 4. DCNMS system configuration.

the computer, the computer will generate a signal to the central alarm station indicating there is a request to put an area into access. The command from the central alarm station is sent to the local SCADA MUX, and the alarms will be masked from that area at the multiplexor.

Reliability and Error Considerations

Field Concentrator

With the exception of the field concentrator, all components of the LORAX system are redundant. Back-up emergency power is provided to all system components. While the multiplexor provides a single point of failure, design of the system is such that if a specific multiplexor goes down, the area it collects data from will be sufficiently small so it can be patrolled by a guard during the downtime. The MTBF of the multiplexor indicates we can expect one failure every 7 years per multiplexor.

Communications

The communication system (Fig 4) from the alarm-protected area to the central alarm station consists of redundant phone lines, or in some cases, one line may be coaxial cable. The modems at the multiplexor are redundant and switching is provided so that digital or analog loopback can be controlled from the Tech Control Center at the central alarm station.

The redundant communication lines come in through dual modems at the central alarm station into two different asynchronous controllers into different Tandem computers. All data, both in the multiplexor and the central computer system, are buffered to prevent lost data during any transmission failure. The redundant communication lines from the central alarm station to the operator stations are interfaced to a special piece of hardware that provides the security checking. In the event an operator's terminal should go down, a back-up terminal is provided at the central alarm station for the dispatching of alarms.

Central Computer System

The central computer system is comprised of three Tandem 16 computers. The ability to continuously monitor and process security information on line can be achieved by this multiprocessor system specifically designed to incorporate the hardware and software features necessary for nonstop operation.

The Tandem 16 system includes the following hardware items:

- All hardware modules are duplicated
- Hardware failure of one module does not affect others
- Multiple paths between all modules
- No critical power supplies in the system
- Very high intermodule transfer rates (to avoid excessive overhead involved in keeping all modules updated with the current system status)
- Repairs are effected without shutting down the system
- Use of conventional circuitry
- Hardware modules are available off the shelf

The software factors include the following:

- A multiprocessor operating system
- An operating system capable of changing message routes (on behalf of the application programs) to avoid failed components
- An operating system capable of reconfiguring itself "on the fly"

- No critical processors (system masters) are included that can corrupt the system
- The failure handling and recovery is not left to the application programmer
- The application programs can be written independently of system configuration in a block structural language.

Central Alarm Station Power

The power system for the central alarm station consists of normal utility power, which in turn is backed up by a 30-minute uninterruptible power supply (UPS) system, which in turn is backed up by a diesel-powered electric generating system. The operator's terminals at Station 100 are all backed up under UPS and diesel-generated power.

Reliability.

An extensive reliability analysis has been conducted on the redundant parts of the system, and results have shown that the system should be able to process alarms 99.997% of the time exclusive of field concentrator downtime.

As stated previously, all data are buffered and require an acknowledgment transmission before the buffers can be cleared. Each transmission is accompanied by a 16-bit CRC check.

Conclusions

The LORAX system provides a sophisticated, distributed intelligence alarm system achieved through the use of a conservative approach.

Each piece of hardware, while using state-of-the-art technology, has been proved in previous installations; the software being generated to tie the system together is structured such that expansions and changes can be easily handled. All system generations can be handled while the system is on line with only a momentary interruption during changeover to the new configuration.

The LORAX system is scheduled to be operational during the summer of CY-81 and will provide a flexibility and expansion of use not obtainable with present off-the-shelf alarm systems.

Reference

1. Robert DesJardin, "The Los Alamos Scientific Laboratory Long-Range Alarm System," Proc. 1979 Carnahan Conference on Crime Countermeasures, Lexington, Kentucky, May 14-16, 1980.